IN THE CLAIMS

No claims have been amended. A copy of the claims is set forth for ease of examination.

1. - 3. (Canceled)

4. (Previously Presented) A method comprising:

selectively auditing a number of transactions between a wireless computing device and a server based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the wireless computing device.

5. (Previously Presented) The method of claim 4, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless computing device; and

encrypting the audit log based on an encryption key that is generated and stored within the wireless computing device.

6. (Previously Presented) The method of claim 4, wherein securely storing the at least one attribute comprises:

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the wireless computing device.

7. (Original) The method of claim 6, wherein securely storing the at least one attribute comprises:

incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log.

8. (Original) The method of claim 4, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

9. - 29. (Canceled)

30. (Previously Presented) A machine-readable medium that provides instructions, which when executed by a wireless device, cause said machine to perform operations comprising:

selectively auditing a number of transactions between the wireless device and a server based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the wireless device.

31. (Previously Presented) The machine-readable medium of claim 30, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless device; and

encrypting the audit log based on an encryption key that is generated and stored within the wireless device.

32. (Previously Presented) The machine-readable medium of claim 30, wherein securely storing the at least one attribute comprises:

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the wireless device.

33. (Original) The machine-readable medium of claim 32, wherein securely storing the at least one attribute comprises:

incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log.

34. - 36. (Canceled)

37. (Previously Presented) The method of claim 4, wherein selectively auditing of the number of transactions includes opening an audit session upon receipt of one of the selected audited transactions, wherein securely storing the at least one attribute of one of the selected audited transactions includes storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless device.

38. (Previously Presented) The method of claim 37, wherein selectively auditing of the number of transactions further comprises:

closing the audit session; and

generating a hash of the audit log after the audit session is closed.

39. (Previously Presented) The method of claim 38, wherein selectively auditing of the number of transactions further comprises generating a digital signature of the hash based a first encryption key, after the audit session is closed.

40. (Previously Presented) The method of claim 39, wherein selectively auditing of the number of transactions further comprises storing the hash and the digital signature in the audit log, after the audit session is closed.

41. (Previously Presented) The method of claim 40, wherein selectively auditing of the number of transactions further comprises encrypting the at least one attribute with a second encryption key, after the audit session is closed.

42. (Previously Presented) The method of claim 41, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

43. (Previously Presented) The machine-readable medium of claim 30, wherein selectively auditing of the number of transactions includes opening an audit session upon receipt of one of the selected audited transactions, wherein securely storing the at least one attribute of one of the selected audited transactions includes storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless device.

44. (Previously Presented) The machine-readable medium of claim 43, wherein selectively auditing of the number of transactions further comprises:

closing the audit session; and

generating a hash of the audit log after the audit session is closed.

45. (Previously Presented) The machine-readable medium of claim 44, wherein selectively auditing of the number of transactions further comprises generating a digital signature of the hash based a first encryption key, after the audit session is closed.

46. (Previously Presented) The machine-readable medium of claim 45, wherein selectively auditing of the number of transactions further comprises storing the hash and the digital signature in the audit log, after the audit session is closed.

47. (Previously Presented) The machine-readable medium of claim 46, wherein selectively auditing of the number of transactions further comprises encrypting the at least one attribute with a second encryption key, after the audit session is closed.

48. (Previously Presented) The machine-readable medium of claim 47, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

49. (Previously Presented) The method of claim 5, wherein the encryption key is stored within a memory within a cryptographic processing module of the wireless computing device.

50. (Previously Presented) The method of claim 5, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing the encrypted audit log in a memory of a cryptographic processing module in the wireless computing device which performed the encrypting, in response to a determination that an audit session that includes the number of audit transactions is a high-valued audit session; and

storing the encrypted audit log in a memory that is external to the cryptographic processing module, in response to a determination that the audit session is not a high-value audit session.